# Security in Internet of Things: A comprehensivereview of Simulators, Emulators and Test-beds

**Nilutpol Bora**

*Information Technology Delhi Technological University*
Delhi, India pnilut@gmail.com

**Himanshu Nandanwar**

*Information Technology Delhi Technological University*
Delhi, India himanshunandanwar9cm0@gmail.com

**Anamika Chauhan**

*Information Technology Delhi Technological University*
Delhi, India anamika@dtu.ac.in

Abstract—The term Internet of Things is seen to be gaining more attention, thanks to the added convenience factor of automating tedious tasks, and much wider area of applications with the boom of internet-based services over the recent years. These IoT based systems market has seen tremendous growth whether it be end-to-end IoT services, or systems having an underlying IoT structure, due to its broad applicability. The IoT field being an amalgam of various other existing fields as wireless networks, network security, internet, related hardware, etc., making it challenging for researchers as they need to work both with the physical as well as soft aspect of it, even so with providing security to them. The evolving hardware components and related firmware, the researchers need to keep exploring better IoT solutions to cope with the pace of these advancements. However, any proposed solution needs to be verified, which can be exhausting when a single vulnerability to the solution can affect millions of interlinked devices. The researchers require a suitable environment for creating an efficient solution, simulation of the IoT network is one such viable approach that can help the researchers in deciding the more appropriate techniques, analyse the short comings of the network as well as improve the system more easily and effectively. This paper has presented a comprehensive review of various tools/frameworks for sim- ulations in the field of security for IoT (Internet of Things), highlighting the importance of simulations, for testing/ evaluating the researchers proposed studies, so as to help researchers enhance the understanding of IoT simulation tools to make an informed choice.

Index Terms—IoT applications, security, Simulators, Emula- tors, Test-beds

## I. INTRODUCTION

One of the major reasons for the growth of IoT based devices market and the success it found over the past decade is the added convenience and the benefits of internet-based services. With the current generation inclined over the conve- nient lifestyle, that these devices offer, exponential expansion of IoT field was eminent, which shifted the focus of

many researchers on studies for better IoT algorithms, protocols, or techniques. These interlinked physical devices usually provide some particular use case functionality to the user based on the data gathered over the sensors, however given there are no set standards for the IoT communication protocols, their varied deployment standards, configurations, software, power management systems, etc., there lies an underlying problem for the testers. With infinite number of possible combinations of sensors and architectures designing a universal testing framework can be a tedious task, added to which some scenes may require over a million such connected devices. Using the traditional testing scenarios may not be viable solution at the present times, when the IoT devices are used in critical sectors as healthcare, surveillances, military, etc. validating the IoT system reliability will be a major area of interest.

Researchers have brought forward the idea of using sim- ulations for such tasks, where this concept is nothing new, as multiple generic network simulators have been in the market for decades, the main focus is on the frameworks for simulations built for IoT based devices. These system architectures are quite similar yet differing in nature from the generic network devices, in terms of functionality, point of operations, etc., simulation frameworks or tools helps in simulating the IoT networks, making designing and testing re- liability of the system more practical. One of the key concerns, nonetheless remains is securing the IoT network, even though these devices make the lives of user more convenient, it comes at the cost of tedious amount of data, every so often sensitive information on the individual or the company which makes it a possible point of vulnerability. Even with multiple studies proposing various security techniques as the applicability of it cannot be comprehended primarily on the basis of the theories contemplated. In such scenarios a feasible solution can be the virtual testing of a simulated real-world scenarios which helps in analysing for any possible loopholes beforehand, when even a minute security gap that is exploited can become fatal when millions of such devices are being interlinked at any given timeframe.

To explore on this simulation field in aspect of IoT security, this paper presents a review of various available simulation tools frameworks and their discussed on different parameters. This study aims at helping researchers and developers in choosing a better suited tool or framework according to their needs.

## II. BACKGROUND

### *A. Internet of Things*

As per the definition, an IoT (Internet of Things) is the interlinked set of devices to implement some functionality to them by transferring data over the internet, for say fitness

band worn by a user keeps track of various health related parameters as heart rate, steps, etc. is an example of IoT where the band is generating continuous data to provide some specific functionality in this case, keeps track of users health. On that account, IoT is the system of devices generating data, analysing it to trigger a relevant action.

*1) Characteristics of IoT:* The Internet of Things can also be described by its characteristics, as connectivity, actions, integration, analysis/intelligence [19] which are

described as follows:

- Connectivity: In the context of IoT, the link betweenthe devices themselves as well as the internet plays a significant role for the system, relying heavily on the data and its availability at all times for its efficient functionality.

- Things (Sensors/Actuators): The devices or things in an IoT system are what all that can be generate data that can be used to provide some specific functionality and produce some resulting task to the environment based on data.

- Intelligence: As the IoT system is heavily dependent on the data, let it be the data generated by the sensors, or exhausted by the user, it is critical to extract meaningful data from created data. A sensor, that creates data, is onlymeaningful if it is correctly analysed and used to add to its productivity.

- Action: Action can be considered as the meaningful outcome performed by the system in response to theintelligence.

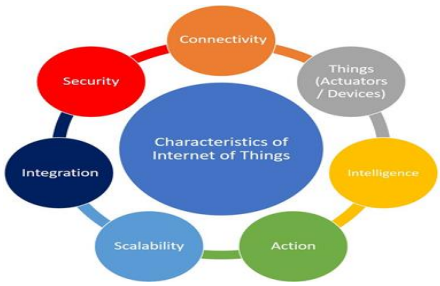
- Scalability: There is no uncertainty on the coming expan-sion of the IoT market, to cope up with it an IoT structure should be able to handle this tremendous increase. The amount of data created as a result is massive, and there must be prior planning for handling it properly.

- Integration: Integration of physical devices and sensors with the environment to allow the user to enhance its experience. It is crucial to integrate the system in order to improve the practicality of the system, which is one of the major reasons for the booming IoT businesses.

- Security: When even a minute security gap that is ex- ploited can become fatal when millions of such devices are being interlinked at any given timeframe, it is impor- tant to focus on the security of the IoT systems.

*2) Applications of IoT:* Internet of Things have been rele- vant in today's world, where it has found its applicability in wide range of sectors, as smart homes, wearables, industry, and many more. Providing the convenience factor to various tedious tasks, and adaptability to different sectors, made the users to choose this technology to automate their tasks [21]. The major sectors utilizing this technology is briefed belowas follows:

- Smart Homes: IoT devices as smart speakers, bulbs, television, etc. have made life more convenient for auser at their home leading to wide spread usage of this technology.




- Fig. 1. Characteristics of IoT

- Wearables: These are small and economically viable wearable devices, which are embedded with sensors, for collecting various measurements as heart rate, oxygen levels, step count, etc., for better understanding of func- tionality of the user.

- Transportation: Traffic, cargo monitoring, electronic ve- hicles uses IoT systems where various sensors provides the system, data for more secure and efficient usage of transportation services.

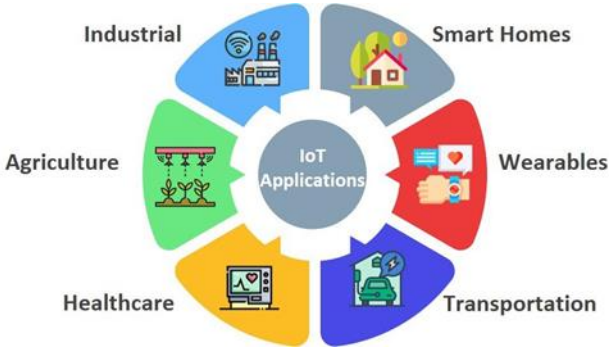



Fig. 2. Applications of IoT

- Healthcare: In this sector, the application of IoT tech- nology can be seen in patient monitoring systems, tohelp better analysis of patient current vitals, medical equipment, etc.

- Agriculture: Monitoring crops and livestock health and requirements at real time has been made possible withthe IoT devices in agricultural sector.

- Industrial: Industrial sector uses IoT systems for monitor- ing the different levels of the manufacturing, processing processes where this data can be used for optimizing the process for increased efficiency.

### *B. Need for IoT simulation*

With the advances in IoT technology and its improved accessibility made the IoT based devices market thrive now more than ever. However, with this new booming market, the companies have been facing the problem of substantiating the device's reliability, with more than millions of linked devices working simultaneously ensuring their expected performances is challenging when there are no set standards for testing strategy with a vast variety of IoT devices available. An IoT device which can range over healthcare devices, industrial equipment, smart homes, toys, etc. not necessarily following the same set of protocols, traditional approaches of testing over sets of input and validating the outputs becomes inefficient. Having varying combinations of sensors data and architectures can generate near impossible sets of testing inputs. Some ofthe key challenges in this are:

- Connecting and implementing a universal testing casescenario for multiprotocol devices can be challengingwhen the market for IoT based devices are ever evolving.

- Different devices in the market uses different deployment standards, configurations,

software, power management systems, etc. which make a hardware-based simulation difficult.

- Testing thousands of linked devices in an IoT architecture for security vulnerabilities is a challenge when the cost of missing them could be very dangerous.

The complex and scalable nature of an IoT infrastructure needs to provide a comprehensive yet flexible approach to test the performance metric of such systems. This is where the virtual testing environments can come handy for IoT systems. A simulated real-world scenario capable of handling multiple linked devices, of varying protocols, can help assist solving these challenges. In this paper we have discussed different tools and platforms available in the market be open sourced, or commercially available, and the different evaluations performed on them by various researchers.

## III. LITERATURE SURVEY

### A. *Attacks on IoT systems*

With explosive growth of IoT field, the focus on research for better IoT algorithms, protocols, or techniques have been more prominent now than ever, where one such area of interest has been the security-based aspect of the IoT. The various attacks prominent in the field of IoT (Internet of Things), as shown in figure 3.

- Physical Attacks: The physical attacks can be regarded as the threats that exploits the systems physical operations. Some of the attacks classified as physical attacks are as micro-probing, reverse engineering, sensor capture, phys- ical communication channel tapping, physical damaging, etc.

- Side Channel Attacks: Side channels attacks are catego- rized as the attacks that does not exploit the program directly rather gathers information on working of the system, and this information is used to compromise the system. Some of the attacks classified as side channels attacks are as time, power, fault analysis, DoS, false node injection, etc.

- Cryptanalysis attacks: These attacks are classified as the attacks that makes use of nature and characteristics of a cryptographic technique used to secure the system. Cypher-text only, known/ chosen plain text, man-in-the- middle attacks, key hijacking, brute force attacks are some of the cryptanalysis attacks.


Fig. 3. Security attacks in IoT system

- Software Attacks: Attacks that tries to gain access on IoT devices in order to run malicious code to inhibit proper functioning of the system. Viruses, worms, trojans, malwares are some of the examples of software attacks.

- Network Attacks: The attacks targeting the sensors net- work to gain unauthorized access of the IoT network are classified under network attacks. Routing attacks, sniffing, flooding, sinkhole, blackhole, packet cloning, aresome of the examples of network attacks.

- Data Attacks: Data attacks can be regarded as the attacks that targets the IoT systems data, more specifically sensi- tive information. Data corruption, modification, DoS, etc. are some of the data attacks.

### *B. Tools for end-to-end simulations in IoT security domain*

The focus on research for better IoT algorithms, protocols, or techniques have been more prominent now than ever, however, such researches are not always viable to implement using the traditional hardware, countering which solutions based on simulations, multiple tools have been proposed over the years to simulate the process on a virtual environment to back up the theories proposed by the researchers.

One of the key concerns, nonetheless remains is securing the IoT network even with multiple studies proposing various security techniques as the applicability of it cannot be com- prehended primarily on the basis of the theories contemplated. In such scenarios a feasible solution can be the virtual testing of a simulated real-world scenarios, for which Patel et al., [2] carried out a comprehensive review comparing such different tools available for IoT over different parameters and broadly classified them over simulators, emulators, and testbeds.

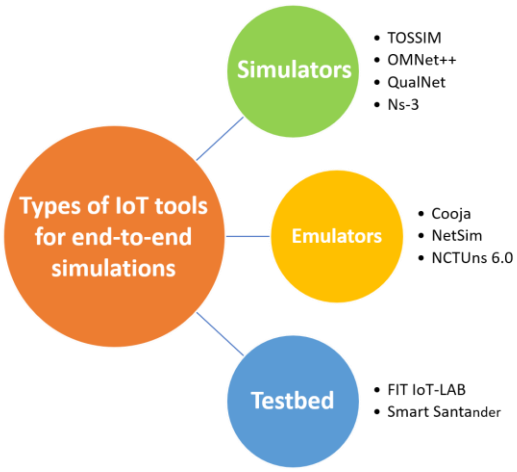



Fig. 4. Types of IoT tools for end-to-end simulations

In this section, the different IoT tools that were found tobe focusing on the security field of IoT are discussed briefly. The section is categorised as IoT simulators, emulators and testbeds, where the tools are briefed and related studies are analysed as to what different

IoT tools provide in context of security. This comparison aims to help researchers and developers in choosing a better suited tool according to their needs.

*1) Simulators:*

- *NS-3:* The NS-3 is a network simulator designed typ- ically for the research community; the simulator can be used for wide range of simulations for replicating the perceptual layer of IoT. Being a network simulator, it lacks some features for simulating the networks for IoT, though the support can be added through manual extensions. NS-series simulators though mainly seen for modelling generic network structures, in recent studies IoT simulations were also observed as Wu et al. [17] used to simulate their work on intrusion detection systems where they were able to detect as well as trace malicious nodes in the network, where the model proposed was focused on detecting energy exhaustion attacks on a 240 node IoT network modelled on NS-3. MANET based IoT was also simulated in a study by Siddiqui et al. [4], to analyze the affects of blackhole and wormhole attacks on a low powered IoT network, this models reliability was supported by the simulations performed on a NS-3 modelled network of 7 and 15 nodes respectively.

- *OMNeT++:* OMNeT++ is a free non-commercial simula- tion tool majorly used for building network simulations. Some of the papers that used this tool in their research implementation were seen as in simulating DDoS detec- tion in IoT, where Alnuman et al. [8] used OMNeT++ to represent a 100-node home network to evaluate their algorithms accuracy. In another paper by Gupta et al.

[5] blockchain applicability in IoT to secure the data transmission was also simulated using this tool, this approach was tested on a 40 node IoT network to simulate the process of data communication. However, one of the concerns is the limited number of built-in protocols supported, which can be solved by using various manual extensions available according to the user needs.

- *QualNet:* The QualNet simulator is a commercial version of Glomosim, primarily supporting built-in ZigBee proto- col. IoT security-based papers where QualNet was imple- mented were as Ahuja et al. [18] where the authors stud- ied the effect of wormhole attack on routing protocols on a 50 node IoT network to support their proposed model. Apart from intrusion detections, researchers have also used QualNet for performance analysis, as Govindasamy et al. [7] proposed a study comparing the performance of different hybrid routing protocol in IoT and verified their stance by simulating them in a 50 node IoT network in QualNet simulator.

- *TOSSIM:* TOSSIM is an IoT (Internet of Things) simu- lator designed primarily for simulations of TinyOS smart devices. Even though TOSSIM is majorly used to sim- ulate TinyOS applications, still some researches where TOSSIM was implemented in security field for internet of things one such study by Sedjelmaci [9] follows anomaly detection techniques in low-resource IoT devices and the proposed model was simulated on a 300 node IoT network using the TOSSIM simulator.

*2) Emulators:*

- *Cooja:* Cooja is an emulator that is accessible in the Contiki operating system (OS), which is one of the more popular OSs for programming IoT sensors. This makes modelling a network for IoT is much easier thanks to the access of majority of standards and protocols provided by Contiki, allowing researchers to recreate or model sim- ulations faster. Another point for researchers to consider Cooja is the ability to directly transfer simulations to physical models with minimum efforts. Cooja was seen to be implemented in multiple studies to create the virtual network model, where researchers used it to support their work in the IoT security as; intrusion detection systems for Internet of Things network were proposed by Ioulianou et al. [3] for DoS attacks detections which was designed using Cooja and evaluated on 7 node IoT network; Anhtuan et al. [6] for routing attacks detection on a 100 node IoT network; and a deep learning-based monitoring of routing protocol attacks by Yavuz et al[10], where the study validated their results on a large scale 1000 node IoT network modelled on Cooja.

- *NetSim:* NetSim is an IoT (Internet of Things) network emulation tool for protocol simulation and security appli-

TABLE I

TOOLS FOR END-TO-END SIMULATIONS IN IOT SECURITY DOMAIN

| **Tools/ Platform** | **Refd. paper** | **Year** | **Scope of paper** | **Type of network** | **Attacks** | **Paper description** |
|---|---|---|---|---|---|---|
| **Simulators** | | | | | | |
| **Ns-3** | Siddiqui et al. [4] | 2021 | Performance Analysis | 7,15 MANET Based IoT | Blackhole and Wormhole Attack | compared the network affectibility under attack using NS-3 |
| | Wu et al. [17] | 2020 | Intrusion Detection on constrained resources | 240 node IoT network | Energy Exhaustion Attacks | hybrid IDS for IoT, experiments performed on NS-3 |
| **OMNet++** | Gupta et al. [5] | 2018 | ensure security of data communicatio n | 40 node IoT network | N/A | Blockchain consensus model for data transmission, evaluation on OMNet++ |
| | Alnuman et al. [8] | 2020 | DDoS detection | 100 node IoT network | DDoS | Machine learning based DDoS detection, validation on OMNet++ |
| **QualNet** | Govindasam y et al. [7] | 2018 | Performance Analysis | 50 node IoT network | Wormhole Attacks | Analysis of various routing techniques in presence of wormhole attacks |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Almomani et al. [18] | 2017 | Performance analysis | 50 node IoT network | N/A | Implementation and performance analysis of proposed routing protocol in Qualnet |
| **TOSSIM** | Sedjelmaci et al. [9] | 2016 | Anomaly Detection | 300 node IoT network | DoS | Lightweight anomaly detection for IoT, demonstrated the viability using TOSSIM |
| **Emulators** | | | | | | |
| **Cooja** | Ioulianou et al. [3] | 2018 | Intrusion detection | 7 node IoT network | DoS | Signature-based IDS for IoT, and evaluated on Cooja |
| | Aiash et al. [6] | 2016 | Specification-based IDS | 100 node IoT network | RPL topology attack | Intrusion detection for RPL based network, validated on Cooja |
| | Yavuz et al. [10] | 2018 | Routing attack detection | 1000 node IoT network | Decreased Rank, Hello Flood, Version Number | deep-learning based continuous security monitoring analysis for IoT |
| **NetSim** | Prasadh et al. [20] | 2019 | Efficiency Analysis | 10 node IoT network | Jamming attacks | Anti-jamming techniques efficiency were analyzed on NetSim network |
| | Remesh et al. [11] | 2020 | Intrusion Detection | IoT network | DoS, DDoS, Botnet | Network performance was analyzed using NetSim during intrusions |
| **NCTUns 6.0** | Saeedi et al. [12] | 2019 | DDoS detection and mitigation | IoT network | DDoS | Proposed machine learning based model was tested in emulator |
| **Test-Beds** | | | | | | |
| **Fit-IoT lab** | Antonio et al. [14] | 2020 | RPL security improvement | IoT Test-bed | N/A | Evaluation of security mechanisms in RPL protocol and experimental analysis on testbed |
| | Khadr et al. [15] | 2020 | Performance validation | IoT Test-bed | Jamming attacks | Performance validation of proposed model for CR-IoT applications under jamming attacks performed on |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | testbed |
| **Smart Santander** | Sidra et al. [16] | 2016 | Security threats analysis in smart city | IoT Test-bed | Physical, data, software attacks | Various security threats and possible solutions in the testbed based smart city were analyzed |

cations. It covers a wide range of protocols for simulating IoT devices, and sensor networks. NetSim was seen to be implemented in various studies to create the virtual network model, where researchers used it to support their work. Regarding the security in IoT, intrusion detection systems were proposed by researchers as Prasadh et al. [20], where efficiency of anti-jamming techniques proposed were analyzed using the NetSim before and after the attacks to compare the affect of attacks on a 10 node IoT network; in another paper by Athira et al., [11] proposed an architecture for detecting DoS, DDoS, and botnet attacks, which was evaluated using NetSim and the impact of these attacks on the network was analyzed.

- *NCTUns 6.0:* NCTUns 6.0 is an open-source network simulator cum emulator. It was seen to be implemented in various studies to create the virtual network model, where researchers used it to support their work. Regarding the security in IoT, intrusion detection systems were proposed by researchers as Kubra et al., [12] to evaluate their DDoS detection model; Grover et al., [13] implemented a multiple misbehaviour detection model VANET and experiments were performed in NCTUns with various VANET simulation scenario.

*3) Testbeds:*

- *FIT IoT-LAB:* FIT IoT-LAB is one of the more popular experimental test-bed for testing out a wide scale IoT or embedded device. The testing environment features more than 200 mobile robots and 3000 IoT nodes. It was seen to be implemented in various studies to solidify the proposal, in terms of the security in IoT, Antonio et al.,

[14] proposed improvement of RPL security scalability and used FIT IoT-Lab for the experiments to evaluate the efficiency of the proposed technique. Another study by Khadr et al., [15] used FIT IoT-LAB to validate their algorithm against jamming attacks on IoT devices.

- *SmartSantander:* SmartSantander is a testbed for eval- uating IoT applications in smart city field. Consisting of more than 20000 IoT devices having sensor nodes, RFIDs, etc. is one of the biggest testbeds for smart city domain. The major advantage of SmartSantander is the variety of sensors that allows researchers from different area of interest in IoT can make use of the testbed. It was seen to be implemented in various studies majorly in smart city-based research. Regarding the security, Shah et al., [16] conducted a thorough review over the SmartSantander testbed security concerns and proposed the viable solutions to them.

## IV. DISCUSSION

The various simulations tools/frameworks used in the secu- rity domains of IoT (Internet of

Things) have been discussed and related studies have been explored, categorizing them into simulators, emulators and test-beds. The choice of the framework to be used by the researcher for their study, whether it be a simulator, emulator or test-bed depends upon the IoT system, the level of simulation required by them.

A simulator can be used for Internet of Things research based on the scope of the study, i.e., it is better suited for studies where an initial abstract model of the IoT network is adequate. Instead of a complex physical system of IoT devices, a simulator is used to design a much ideal model of the IoT network much easily and effectively. These models help researchers quickly design the proposed architecture or technique and analyse the logic flow and if the proposed theory is actually a viable solution that should be developed further for deployment, that is simulators are useful as a proof-of- concept tool. An IoT network simulated in a simulator helps to figure any semantic flaw in the algorithm, which can reduce wastage of resources. As in case of a real hardware imple- mentation of a multi node IoT network to test a theoretical approach can lead to greater expenditure of resources, which could be prevented using a simulator. However, the results from simulators are very much an ideal scenario and hence are not always a reliable standard for determining the performance of this model deployed in a real-world scenario.

A better alternative for researchers to look for if the focus is toward creating simulations closer to practical networks as well as features the advantages of simulators as configurability, scalability, control of the network, the middle ground could be the emulators. An emulator maps real IoT devices to corresponding simulated devices, executing parallel to real Internet of Things nodes. This helps researchers to port their IoT system or architecture directly to real world IoT system with minimal changes, even so the results produced from simulations in an emulator are more reliable than those of a simulator.

While both simulators and emulators are helpful when researchers are working limited scope or are in the initial stages of development of IoT system, the researchers working in the later stages, they expect results that are more practical to better optimize their systems for real world. The IoT test beds are the better alternative to simulators and emulators when it is not viable for physical IoT devices yet they require more reliable experimentation results. These test-beds provides access to researchers to a variety of readily accessible IoT network to conduct their experiments. However, they lack the configurability, scalability, control over the network as in case of simulators and emulators.

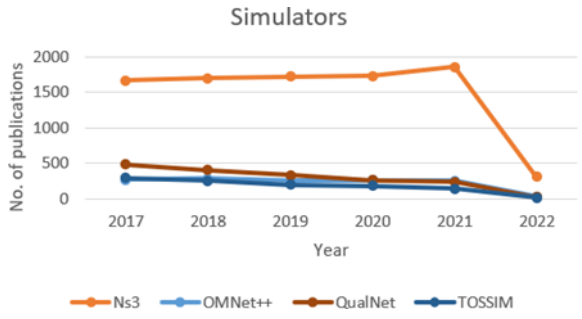



Fig. 5. Papers published on IoT simulators

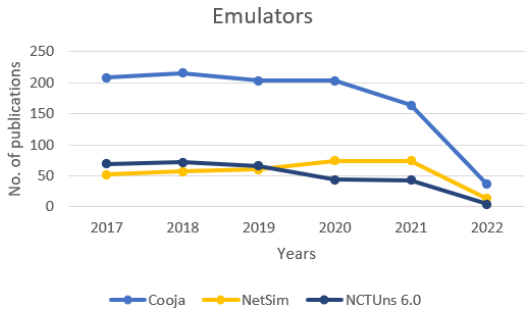



Fig. 6. Papers published on IoT emulators

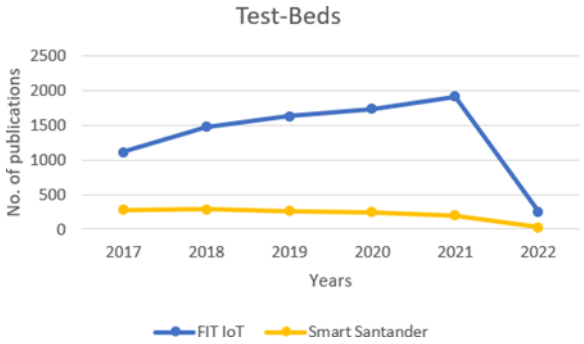



Fig. 7. Papers published on IoT test-beds

The IoT field is the amalgam of various other existing sectors as wireless networks, network security, internet, related hardware, etc., making it challenging for researchers as they need to work both with the physical as well as soft aspect of it. The simulations of the IoT networks helps the researchers in deciding the more appropriate techniques, analyse the short comings of the network as well as improve the system more easily and effectively. To show the shift of researchers towards the use of simulations in Internet of Things, figure 5,6, and 7 shows the number of publications of the various simulation tools discussed in this paper over the past 6 years.

## V. CONCLUSION

This study has presented a comprehensive review of vari- ous tools/frameworks for simulations in the field of security for IoT (Internet of Things), highlighting the importance of simulations, for testing/ evaluating the researchers proposed studies. There have been various simulations tools for generic computer networks in the past, however even though IoT networks share similarities with such networks, these tools can not be assumed to perform the same with those of IoT network devices, where devices varies widely over deployment standards, configurations, softwares, power systems.

In this paper, we have classified these simulation tools/ frameworks into three categories simulators, emulators and test-beds and presented a survey of various security implementation papers in the field of Internet of Things. These tools have been analysed where they have been discussed according to the scope of the IoT studies to help researchers choose a better suited tool for their needs.

## REFERENCES


[1] Verma, Abhishek, and Virender Ranga. "ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things." In 2019 4th International conference on Internet of Things: Smart innovation and usages (IoT-SIU), pp. 1-6. IEEE, 2019.

[2] Patel, N. D., B. M. Mehtre, and Rajeev Wankar. "Simulators, emulators, and test-beds for internet of things: A Comparison." In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 139-145. IEEE, 2019.

[3] Ioulianou, Philokypros, Vasileios Vasilakis, Ioannis Moscholios, and Michael Logothetis. "A signature-based intrusion detection system for the Internet of Things." Information and Communication Technology Form (2018).

[4] Siddiqui, Muhammad Nasir, Kaleem Razzaq Malik, and Tauqeer Safdar Malik. "Performance analysis of blackhole and wormhole attack in MANET based IoT." In 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), pp. 1-8. IEEE, 2021.

[5] Gupta, Yash, Rajeev Shorey, Devadatta Kulkarni, and Jeffrey Tew. "The applicability of blockchain in the Internet of Things." In 2018 10th International Conference on Communication Systems & Networks (COMSNETS), pp. 561-564. IEEE, 2018.

[6] A. Le, J. Loo, K. K. Chai, M. Aiash, A specification-based IDS for detecting attacks on RPL-based network topology, Information 7 (2) (2016) 25.

[7] Govindasamy, Jegan, and Samundiswary Punniakody. "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack." Journal of Electrical Systems and Information Technology 5, no. 3 (2018): 735-744.

[8] Alnuman, Ibrahim Ahmed, and Mousa Al-Akhras. "Machine learning DDos detection for generated internet of things dataset (IoT Dat)." In 2020 2nd International Conference on Computer and Information Sciences (ICCIS), pp. 1-6. IEEE, 2020.

[9] Sedjelmaci, Hichem, Sidi Mohammed Senouci, and Mohamad Al- Bahri. "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology." In 2016 IEEE international conference on communications (ICC), pp. 1-6. IEEE, 2016.

[10] Yavuz, Furkan Yusuf. "Deep learning in cyber security for internet of things." Master's thesis, Fen Bilimleri Enstitüsü, 2018.

[11] Remesh, Athira, Divya Muralidharan, Neha Raj, J. Gopika, and P. K. Binu. "Intrusion detection system for IoT devices." In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 826-830. IEEE, 2020.

[12] Saeedi, Kubra. "Machine learning for ddos detection in packet core network for iot." (2019).

[13] Grover, Jyoti, Nitesh Kumar Prajapati, Vijay Laxmi, and Manoj Singh Gaur. "Machine learning approach for multiple misbehavior detection in VANET." In International conference on advances in computing and communications, pp. 644-653. Springer, Berlin, Heidelberg, 2011.

[14] Arena, Antonio, Pericle Perazzo, Carlo Vallati, Gianluca Dini, and Giuseppe Anastasi. "Evaluating and improving the scalability of RPL security in the Internet of Things." Computer Communications 151 (2020): 119-132.

[15] Khadr, Monette H., Haythem Bany Salameh, Moussa Ayyash, Sufyan Almajali, and Hany Elgala. "Testbed Validation of Security-Aware Channel Assignment in Cognitive Radio IoT Networks." In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), pp. 1-6. IEEE, 2020.

[16] Ijaz, Sidra, Munam Ali Shah, Abid Khan, and Mansoor Ahmed. "Smart cities: A survey on security concerns." International Journal of Advanced Computer Science and Applications 7, no. 2 (2016): 612-

625.

[17] Wu, Chao, Yuan'an Liu, Fan Wu, Feng Liu, Hui Lu, Wenhao Fan, and Bihua Tang. "A hybrid intrusion detection system for iot applications with constrained resources." International Journal of Digital Crime and Forensics (IJDCF) 12, no. 1 (2020): 109-130.

[18] Almomani, Iman, and Maha Saadeh. "S-FEAR: secure-fuzzy energy aware routing protocol for wireless sensor networks." KSII Transactions on Internet and Information Systems (TIIS) 12, no. 4 (2018): 1436-1457.

[19] Jaidka, Himanshu, Nikhil Sharma, and Rajinder Singh. "Evolution of iot to iiot: Applications & challenges." In Proceedings of the international conference on innovative computing communications (ICICC). 2020.

[20] Prasadh, S. Kshipra, and Sumit Kumar Jindal. "Security and Efficiency Analysis of Anti-jamming Techniques." In International Conference on Internet of Things and Connected Technologies, pp. 251-259. Springer, Cham, 2019.

[21] Nandanwar, Himanshu, and Anamika Chauhan. "IOT based Smart Environment Monitoring Systems: A Key To Smart and Clean Urban Living Spaces." In 2021 Asian Conference on Innovation in Technology (ASIANCON), pp. 1-9. IEEE, 2021.